Ransomware Taxonomy

Ehimare Enaholo ,Mawuli Martey

Department of Information Systems, St. Cloud State University, St. Cloud, MN, United States

Department of Computer Science and Information Technology, St. Cloud State University, St. Cloud, MN, United States

Abstract

Ransomware poses a significant threat to individuals and organizations, causing financial loss, data breaches, and reputational damage. This paper presents a comprehensive taxonomy of ransomware, categorizing it into types such as crypto-ransomware, scareware, and locker ransomware, along with emerging variants like leakware and Ransomware as a Service (RaaS). Through experiments evaluating the taxonomy's usability, we identified strengths such as ease of navigation and consistency, while also noting areas for improvement including the need for descriptive labels and potential column adjustments. Our research underscores the urgency of understanding ransomware and offers insights for refining taxonomies to enhance comprehension and mitigation strategies.

Keywords: Ransomware, Taxonomy, Crypto-Ransomware, Scareware, Locker Ransomware, Leakware, Ransomware as a Service (RaaS)

1. Introduction

The complexity of computers is important to perform many business functions. Sometimes, these functions are more than important; they are completely necessary to organizations, and the people are supported by them. As a result, it becomes attractive to malicious actors who are willing to disrupt these functions and hold them for ransom, often at an extraordinary price.

Ransomware, a form of malicious software, encrypts important files on a user's computer and demands payment to decrypt them and restore access. In recent years, it has emerged as a major cyberthreat that targets not only large corporations but both individuals and organizations. The typical ransomware attack starts with an unsuspecting user clicking on a malicious link or email attachment that appears legitimate. However, this installs a ransomware program allowing cybercriminals remote access to infiltrate the victim's system. The ransomware then secretly begins encrypting files on the hard drive or network using complex algorithms. By the time the user realizes something is wrong, the ransomware displays a message demanding payment to receive the decryption key.

Almost everyone, groups, and entities are susceptible to ransomware. Attacks by ransomware impact a wide range of industries, and their targets are not always the same. Ransomware is not just a technical issue, it's a digital threat with real-world consequences. It can cripple individuals and businesses alike, causing financial loss, data breaches, and reputational damage. It can access things such as Personal Identifiable Information (PII), important documents, halt communications, identity theft, and emotional distress.

Attacks using ransomware have spread throughout the world and now pose a danger to cybersecurity for both individuals and businesses. Because cybercriminals operate globally and take advantage of weaknesses in digital systems, these destructive activities are not restricted to any one area. It is also noteworthy how often ransomware is in industries like healthcare, finance, and key infrastructure.

Many interrelated reasons contribute to the development and longevity of ransomware as a serious Cybersecurity issue. For cybercriminals, these attacks are quite profitable, which is one of the main

motivations. Because ransomware enables attackers to demand huge sums of money from victims without physical contact or direct confrontation, it offers a low-risk, high-reward opportunity. These ransom payments can be requested and paid with cryptocurrencies, thereby adding an extra degree of anonymity, making it more difficult for law authorities to find and capture the offenders.

2. Related Work

Ransomware attacks affect nearly one out of every five businesses. A shocking 21% of respondents said yes to the question, 'Has your organization ever been the target of a ransomware attack?' While this may appear to be a high figure, it lines up with statistics from a previous email security survey the authors did, which revealed that one out of every four businesses had experienced an email security breach. The findings highlight ransomware's enormous frequency, making it one of the most popular - and effective - kinds of cybercrime.

Being a ransomware victim can be disastrous. The average delay a firm lives on after a ransomware attack is 21 days, and the cost of that downtime alone can be deadly for many businesses, even before considering the cost of information recovery, ransom payment, implementing the disaster recovery plan and long-term brand harm. And the ransom is not cheap, with the average sum that businesses ended up having to pay in 2020 at $170,404. The obvious next question is, how many of these ransomware victims paid the ransom to retrieve their data and resume operations? (Ransomware Attacks Survey, n.d.)

After an attack by ransomware, about one out of every ten businesses is forced to pay a ransom to restore data. According to the report, 9.2% of companies who were victims of a ransomware assault were forced to pay the ransom to restore their data. This data demonstrates that, with proper information and precautions, paying the ransom does not have to be the only choice. Despite being attacked, more than 90% of our respondents indicated they were able to restore their data from backup. However, while some people were able to restore their data without paying the ransom, they also lost information in the process, so they couldn't flee unharmed. (Ransomware Attacks Survey, n.d.) 15.2% of organizations do not secure backups from ransomware. Data backups are basically the lifeline of any anti-ransomware approach. If a shared drive has been encrypted by malware, an IT team can retrieve the data from the most recent backup with minimal data loss. Having said that, our survey indicated that more than 17.2% of attacks by ransomware on the survey participants targeted backup data, highlighting a vulnerability that scammers can take advantage of. If a company's backup data is similarly encrypted, it becomes useless as a ransomware security technique. The fact that more than 15% of businesses make no effort to secure their backups from ransomware is troubling. While frequent backups safeguard against other potentially devastating events such as computer crashes, protection from ransomware must also be one of its major functions. Most attacks by ransomware can be avoided if a duplicate backup plan is followed. (Ransomware Attacks Survey, n.d.)15.9% of firms are missing a plan for disaster recovery in place. IT disaster recovery plans (IT DRPs) are a further essential aspect of securing company data from unpredictable dangers. It is critical to be able to provide company continuity in the case of a technological failure. According to the authors' poll, an equivalent number of the participants that fail to secure their backups usually fail to have a plan for disaster recovery in effect. Furthermore, keeping your IT Disaster Recovery Plan up to date protects you from more than simply ransomware assaults. Human mistakes, technology failure, and disasters of nature are all reasons to have effective recovery plans set up that you can deploy quickly to minimize harm. (Ransomware Attacks Survey, n.d.)

According to (Razaulla, et al., 2023), Ransomware, a type of malware that encrypts users' data and demands payment to release it, has emerged as a major cybersecurity issue. Researchers all over the world are actively working to discover techniques to counteract this increasing threat, and their efforts are reflected in a broad and diverse body of research. This brief investigates the most important components of ransomware research, providing insights that go beyond the surface. (Ransomware Attacks Survey, n.d.)

Ransomware Research Taxonomy of (Ransomware Attacks Survey, n.d.): At the heart of this investigation is a complete taxonomy of ransomware research, which is classified as follows:

- Static analysis (viewing malware code) and dynamic analysis (observing its behavior during execution) are two types of analysis. (Ransomware Attacks Survey, n.d.)
- Approaches: This category includes techniques such as machine learning, rule-based analysis, and honeypots. (Ransomware Attacks Survey, n.d.)
- Features: Distinctive characteristics used for identification, such as network traffic patterns, API requests, and file activity. (Ransomware Attacks Survey, n.d.)

Unscrambling the Maze - Detection Techniques: It is critical to detect ransomware before it causes damage. The text highlights some strategies used by researchers:

- ML (machine learning): ML systems excel at detecting known and undiscovered ransomware strains by using their capacity to learn from data and find patterns. (Ransomware Attacks Survey, n.d.)
- Approaches Based on Rules: These use pre-defined rules based on certain ransomware features to provide a quick and efficient detection technique. (Ransomware Attacks Survey, n.d.)
- Approaches Using Decoys: Setting up honeypots, or false systems that look like real ones, might entice attackers, and reveal their strategies. (Ransomware Attacks Survey, n.d.)

Sorting Out the Bad Apples via Classification: Once discovered, ransomware must be classified to comprehend its nature and possible consequences. Here's how researchers do it:

- Machine Learning (ML): Once again, ML is dominant, allowing researchers to classify malware as ransomware or benign, and even identify specific ransomware families. (Ransomware Attacks Survey, n.d.)
- Behavioral Analysis: Investigating the malware's actions and interactions with the system provides useful information for classification. (Ransomware Attacks Survey, n.d.)

Prevention: Constructing Ransomware Defenses: To completely avoid ransomware attacks, proactive measures are required. The article illuminates essential preventative strategies:

- Windows Systems are a potential target due to their extensive use. To protect these systems, research is focusing on techniques such as access control policies and backups. (Ransomware Attacks Survey, n.d.)
- MTD (Moving Target Defense): This method regularly modifies the configuration of a system, making it difficult for attackers to exploit weaknesses. (Ransomware Attacks Survey, n.d.)

When Prevention Fails, Damage Mitigation: Even with strict security procedures in place, ransomware attacks can occur. The text investigates techniques to mitigate the damage:

- Key Escrow: By storing copies of encryption keys in secure locations, data can be recovered without paying the ransom. (Ransomware Attacks Survey, n.d.)
- SDN (Software-Defined Networking): SDN provides centralized control over network traffic, allowing for the detection and blocking of malicious activities. (Ransomware Attacks Survey, n.d.)
- Examining infected systems can disclose the origin and scope of the assault, assisting in incident response and future preventive efforts. (Ransomware Attacks Survey, n.d.)

Predicting future trends and attack patterns is a new area in ransomware research. Researchers can use this proactive strategy to design even more effective responses. (Ransomware Attacks Survey, n.d.)

Finally, countering ransomware necessitates a multi-pronged approach, and continued research is critical in this attempt. This summary should have given you a better grasp of the varied and dynamic environment of ransomware research, allowing you to stay educated and prepared in the face of this emerging danger. (Ransomware Attacks Survey, n.d.)

3. Methodology

The aim of this paper is to use ransomware taxonomy to improve the understanding of ransomware. The taxonomy should be able to organize information in such a way that it supports retrieving specific information, finding related or relevant content, and to overall help in understanding a ransomware situation. Before explaining how the taxonomy will be evaluated, it would be best to first explain the taxonomy.

The taxonomy categorizes different types of ransomwares based on their sources, exploitable technology, level of risks, causes or method of attacks including target platforms. This taxonomy provides a structured framework for understanding and analyzing the diverse landscape of ransomware threats. We reviewed several scholarly articles and drew theoretical analyses including the impact, sources, prevention, and classifications. We have drawn mostly theoretical and practical approaches to classifying ransomware and how institutions could curb attacks. Most of the articles reviewed for this paper did not discuss technological tools to prevent or stop attacks but rather focused on understanding different perspectives of ransomware including how organizational policies, education and awareness could be a major contributing factor in reducing and stopping current and future attacks.

4. Types of ransomwares

Ransomware can be classified into three main types based on its behavior: crypto-ransomware, scareware, and locker ransomware (Faghihi et al., 2021). Crypto ransomware poses a significant threat as it encrypts specific data and files. Recovery of infected data becomes challenging once crypto ransomware successfully encrypts its targets, unless the ransomware employs a weak algorithm (Fernando et al., 2022).

Crypto-Ransomware, being the common form of ransomware, seeks to encrypt vital victim data such as documents, images, and videos while avoiding disruption to fundamental computer operations. Typically, Crypto-Ransomware allows victims to view the catalog of encrypted files and operate the system, yet they encounter an inability to open the specific encrypted files. The data encrypted by contemporary Crypto-Ransomware, employing techniques like AES and RSA, is frequently unrecoverable, given that these encryption methods are nearly irreversible when implemented accurately. (Razaulla et al ,2023).

Scareware ransomware utilizes social engineering tactics to lure victims into paying by displaying false alerts. Also, this type of ransomware tricks users into downloading or purchasing harmful, and at times, ineffective software by presenting alarming messages, typically through pop-up ads (Razaulla et al ,2023). Individuals or organizations who fall for this unintentionally end up installing ransomware on their devices. It is crucial to understand that this ransomware variant doesn't necessarily present an actual threat to its victims (Razaulla et al ,2023).

On the other hand, locker ransomware takes an extreme approach by locking computer systems and targeted devices, restricting user access. Unlike other types, locker ransomware does not encrypt files; removing the malware usually leaves stored data unaffected (Richardson et al., 2017). If removal is impractical, transferring storage devices to different systems is a common method for data recovery. Locker ransomware operates by restricting victims' access to their systems. In most instances, individuals affected by Locker ransomware find themselves limited to viewing either the lock screen or a display featuring instructions for ransom payment. Resolving such ransomware attacks is frequently uncomplicated and can be addressed through actions like rebooting the computer in safe mode or employing an on-demand virus scanner (Razaulla et al ,2023).

Leakware, also recognized as Doxware, is usually a method of creating damage rather than a type of ransomware. It threatens to disclose users' data to the public unless a ransom is paid. The damage caused is usually permanent or irreversible because once data is made public, it becomes accessible to anyone. Organizations such as banks and other organizations dealing with confidential or sensitive information are especially vulnerable to potential targeting through this type of cyberattack.

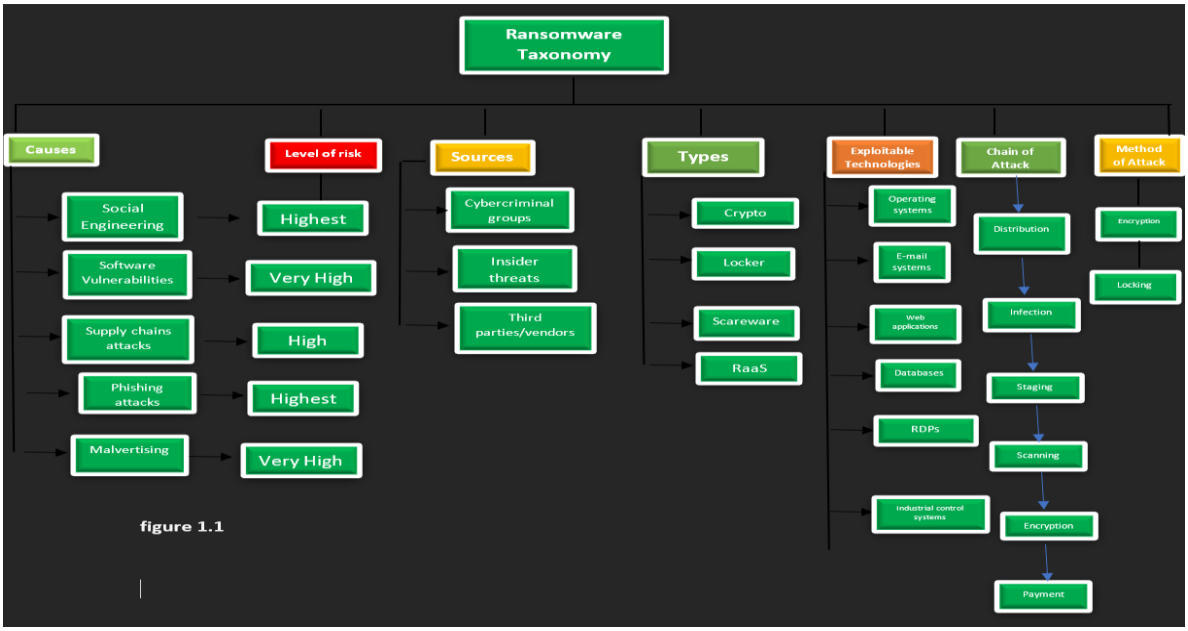
Ransomware as a Service (RaaS) is also a term that is used to refer to how ransomware is distributed. RaaS operates as a distribution model like the Software-as-a-Service (SaaS) model, wherein cyber attackers lease or purchase ransomware attacks to or from fellow cybercriminals. The offerings under this model encompass the ransomware itself, tools for customizing ransomware, and infrastructure for sustaining the ransomware, along with instructional resources. This type of service empowers individuals or cybercriminal groups or script kiddies without the expertise or time to create ransomware to launch

attacks. These are readily available on dark web and illegal websites to purchase on commission or subscription basis.

The existence and fast growth of RaaS could be attributed to many factors especially the advance in technology not excluding machine learning, advanced programming and the availability of malicious plug and play software and source codes. According to Razaulla et al. (2023) "The widespread adoption of the ransomware-as-a-service (RaaS) model has contributed to the steady growth of ransomware attacks in recent years. Several notorious Ransomware-as-a-Service variants exist, including Ryuk, maze, lockbit and Revil, also known as "sodinokibi".

Figure 1

Figure 1 illustrates the ransomware chain. Usually ransomware attacks pass some stages, and it is important to understand these to enable individuals and organizations to prevent, identify or detect and recover from attacks. Distribution is the first or initial stage or phase of ransomware attacks according to some researchers. When organizations identify and stop the distribution of ransomware attacks, it breaks the channel or chain from infection through to payment. The distribution channels which this novel taxonomy identifies as causes or exploitable technology mainly includes phishing through emails especially, infected software or purchase of infected or vulnerable software, vulnerabilities in networks, malicious websites.



This distribution could be exploited through email systems, remote desktops, industrial systems, network protocols etc. as illustrated in figure 2. According to our research we have concluded in our taxonomy that all the causes, method distributions are of high risk but the highest being email systems via targeted phishing attacks. And the best preventive method for this is education, discipline, and awareness creation. Organizational policies or security policies must treat education and awareness and enforcement as high priorities to minimize attacks.

The evaluation of the taxonomy will be done via participants and ransomware scenarios. The participants will be informed of the ransomware scenario and be given relevant facts. The participants should use the information provided by the scenarios to correctly identify which type of ransomware it is. By correctly identifying the correct type of ransomware, we can determine that the taxonomy was a success helping people understand and navigate ransomware scenarios.

The experiments will consist of several 45-second tests. These 45-second tests will consist of a ransomware prompt that should meet many of the points found within the taxonomy. One example prompt can be seen as such:

"Suppose that an elderly couple clicked on an ad as they surfed the internet. A pop-up ad appeared on their screen after clicking the ad, claiming that should they not pay a $100 ransom, they will delete everything on their computer."

The participant would then pick which item within the category correctly aligned with the prompt. Multiple copies of the taxonomy will be available for the participant for them to circle their chosen answers. The aim of this paper is to test the participants 3 times with 3 different prompts of ransomware scenarios.

The purpose of the setup of the experiment is to determine how participants navigate, understand, and use taxonomy. Should the participants successfully use the taxonomy in order to easily understand ransomware, we would consider the taxonomy to be sufficient in organizing, categorizing, and understanding ransomware.

5. Results and Discussions

After the initial tests with the participants, they were asked how they felt utilizing the taxonomy as well as their opinions on other many aspects. They gave several descriptive points as well as feedback on their opinion of the taxonomy with positive and negative opinions.

The participants felt that the taxonomy was easy to navigate. During their testing, they felt it was easy to look for different aspects of the ransomware scenario, as the columns neatly organized the different functions that can be found in a ransomware attack. By looking at the column category, they would easily find related subcategories to describe the scenario.

Another positive aspect was the consistency of the taxonomy. Participants felt that most columns felt in order; that nothing felt as though they didn't belong. This referred to how there was no confusion on how ransomware aspects were categorized. Overall, the opinion was that the taxonomy was well organized in both design and function but felt that its size of the taxonomy and its labels were difficult to read.

Despite its organization, there were negatives to be found in the terms themselves. There were no descriptive aspects applied to the taxonomy, and although these items would be familiar to those who were familiar with business and their vulnerabilities, it was difficult for those who had little to no experience in the subject.

In other cases, they felt that some columns were unnecessary within the ransomware scenario. The 'Level of Risk' column and the 'Chain of Attack' column were unnecessary in describing and categorizing different ransomware scenarios. Though those columns clarify ransomware, they were not utilized effectively by the participants. The feedback by the participants, both positive and negative, help us understand what is essential to a taxonomy and how improvements would occur.

One possible improvement would be to include brief descriptions of items within a column. This would assist greatly in understanding the content ransomware and the many variables within it, as it would quickly determine whether facts about the ransomware scenario are connected to the item.

Another improvement could be the rearrangement or removal of certain columns for better focus and understanding of the taxonomy. While the removal of information would be unideal, it may be necessary to improve navigation and utilization of the overall taxonomy. The removal of such columns would provide quicker times and less confusion during utilization. Alternatively, some columns can be rearranged within the taxonomy to provide a better experience for future participants. Ultimately, a taxonomy should balance information and usability to give the greatest understanding to its users.

6. Conclusions

Ransomware is, as previously mentioned, a significant problem to both individuals and organizations. Whether the ransom be reputational or financial, victims are at the mercy of malicious actors who seek to do harm. Our related work observes how significant the problems of ransomware are exactly and further demonstrating the necessity of finding solutions to understanding ransomware.

One such solution is our proposed taxonomy. This ransomware taxonomy articulates many different aspects of ransomware and is designed to be utilized in a way to support understanding of ransomware. During our experiments, we realized the pros and cons of our taxonomy. We utilized the feedback to pave a way to develop an improved taxonomy in the future. Overall, we find our research into ransomware and our findings on potential solutions to be an important step into further developments.

7. References

Faghihi , F., & Zulkernine, M. (2021). RansomCare: Data-centric detection and mitigation against smartphone cryptoransomware. Elsevier, 191, 1-10. https://doi.org/10.1016/j.comnet.2021.10 8011

Fernando, D. W., & Komninos, N. (2022). Feature selection architecture for ransomware detection under concept drift. Elsevier, 116, 1-13. https://doi.org/10.1016/j.cose.2022.1026 59

Mamoona Humayun, NZ Jhanjhi, Ahmed Alsayat,& Vasaki Ponnusamy,Internet of things and ransomware: Evolution, mitigation, and prevention,Egyptian Informatics Journal,Volume 22,Issue 1,2021, Pages 105-117,ISSN 1110-8665,https://doi.org/10.1016/j.eij.2020.05.003.

Thamer, Noor & Alubady, Raaid. (2021). A Survey of Ransomware Attacks for Healthcare Systems: Risks, Challenges, Solutions and Opportunity of Research. 210-216. 10.1109/BICITS51482.2021.9509877.

Razaulla, S., Fachkha, C., Markarian, C., Gawanmeh, A., Mansoor, W., Fung, B. C., & Assi, C. (2023, 02). The Age of Ransomware: A Survey on the Evolution, Taxonomy, and Research Directions. Retrieved December 2023, from Research Gate: https://www.researchgate.net/publication/370137991_The_Age_of_Ransomware_A_Survey_on_the_Evolution_Taxonomy_and_Research_Directions